I oppose requiring law enforcement access to broadband and VOIP networks due to the additional overhead, cost, and decreased security that this would cause. Any system designed to allow someone (law enforcement) to monitor communications can also allow someone else (hackers) to monitor them; as a potential customer, I would prefer that communications providers be free to design their system to be as secure as possible. Additionally, some more efficient transmission methods and communication designs are unsuitable for wiretapping/monitoring, and others require inefficient and costly technical reworks that degrade the performance of the system to allow this capability. This means that due to a regulatory burden, the network I use (as a customer) will cost more to access, perform worse, and be less secure against hackers. I do not believe this is a positive outcome. Finally, I do not feel on principle that the government has the moral right or compelling interest to demand that all new privately-developed communication methods or networks be easily monitorable by law enforcement. This is an unfeasible demand anyway, as the growing availability of strong encryption tools means that people already have ways to communicate without law enforcement easily monitoring their messages in transit. To ignore this and enforce what will be a more and more useless monitoring requirement, at the cost of network performance and security, is ridiculous. Please do not require broadband or VOIP providers to compromise their networks.